Wie MSPs ihr Geschäft im wachstumsstarken Gesundheitssektor ausbauen können

Cybersicherheit spielt im Gesundheitswesen eine äußerst wichtige Rolle. Denn Systemausfälle und Ausfallzeiten können für die Patient:innen lebensbedrohliche Folgen haben. Leider fällt es vielen Einrichtungen im Gesundheitswesen jedoch schwer, effektive Cybersicherheitsmaßnahmen umzusetzen. Dadurch ergibt sich für Managed Service Provider (MSPs) eine große Chance, ihre Dienstleistungen gewinnbringend anzubieten.

Die Daten des im Jahr 2025 veröffentlichten Berichts von Black Book Market Research verdeutlichen das Ausmaß der Herausforderung:

68 %

der befragten Unternehmen im Gesundheitswesen gaben an, dass sie Cyberrisiken aufgrund unzureichender Mittel nicht angemessen mindern können.

60 %

Fast 60 % der Gesundheitseinrichtungen berichten von Schwierigkeiten bei der Einstellung qualifizierter IT-Fachkräfte und bei deren langfristiger Bindung.

28 %

aller Sicherheitsverletzungen sind auf menschliche Fehler zurückzuführen. Häufigste Ursache sind dabei Phishing-Angriffe.

In der Folge stieg die Nutzung von Managed Security Services im Gesundheitswesen von 2024 bis 2025 um 35 %. Die Geschäftschancen für MSPs sind groß und wachsen weiter.[1]

Warum herkömmliche Managed Services nicht mehr ausreichen

Krankenhäuser sind auf rund um die Uhr verfügbare Systeme wie elektronische Patientenakten, Bildgebungsplattformen und Instrumente zur Patientenüberwachung angewiesen. Fällt eines dieser Systeme aus, hat das direkte Auswirkungen auf die Patientenversorgung. MSPs können mehr als nur herkömmlichen IT-Support bieten. Sie können zu unverzichtbaren Partnern werden, wenn es darum geht, den Betrieb kritischer Systeme aufrechtzuerhalten, die Kontinuität der Patientenversorgung zu gewährleisten und gesetzliche Vorschriften einzuhalten.

Um im Gesundheitswesen erfolgreich zu sein, reichen die üblichen Managed Services jedoch nicht aus. MSPs müssen komplexe regulatorische Anforderungen bewältigen, veraltete medizinische Systeme absichern und Ausfallzeiten nahezu auf null reduzieren können – und das in Umgebungen, in denen jede Minute zählt.

[1] Black Book Market Research, The Black Book of Healthcare Cybersecurity: 2025 Edition

Geschäftliche und technologische Herausforderungen

Erfolg im Gesundheitswesen zu haben, ist nicht leicht. Die Bereitstellung von Services in diesem Sektor ist mit einer Reihe von Herausforderungen verbunden, mit denen viele MSPs möglicherweise nicht vertraut sind. Sie sehen sich einer einzigartigen Kombination aus Betriebsdruck, Sicherheitsrisiken und technischer Komplexität gegenüber.

Auswirkungen von Ausfallzeiten auf die Patientensicherheit

Ausfälle sind im Gesundheitswesen keine Option. Systemausfälle können Behandlungen verzögern, Patienten verlegen und kritische Abläufe in der Patientenversorgung stören. Hinzu kommt, dass Ausfallzeiten kostspielig sind. Laut IBM belaufen sich die durchschnittlichen Kosten einer Datenschutzverletzung im Gesundheitswesen auf 7,42 Mio. USD.[2] MSPs müssen Recovery Time Objectives (RTOs) von nahezu null sowie eine konstant hohe Verfügbarkeit gewährleisten.

Altsysteme vergrößern die Angriffsfläche

Im Gesundheitswesen sind veraltete Infrastrukturen und vernetzte medizinische Geräte nach wie vor allgegenwärtig. Da sich viele dieser Systeme nicht patchen lassen, ohne die Versorgung zu beeinträchtigen, liegt es in der Verantwortung von MSPs, diese veralteten und anfälligen Technologien abzusichern.

Gesundheitsdaten sind für Cyberkriminelle äußerst wertvoll

Geschützte Gesundheitsdaten gehören im Darknet und in kriminellen Kreisen zu den wertvollsten Informationen. Deshalb sind Gesundheitseinrichtungen ein bevorzugtes Ziel für Ransomware-Angriffe und Datendiebstahl. Für MSPs bedeutet das, dass sie einen erweiterten Schutz und eine schnelle Wiederherstellung gewährleisten müssen.

Ransomware nimmt zu

Die Zahl der Ransomware-Angriffe auf das Gesundheitswesen nimmt weiter zu. Laut dem FBI hat sich die Zahl der gemeldeten Vorfälle, bei denen Gesundheitseinrichtungen von Ransomware betroffen waren, von 2024[3] bis 2025[4] um 93 % erhöht. Dabei nutzen Cyberkriminelle die Dringlichkeit des Krankenhausbetriebs gezielt aus. MSPs müssen deshalb einen mehrschichtigen Schutz implementieren, der Prävention, Erkennung und eine zuverlässige Wiederherstellung umfasst.

Komplexe Hybridumgebungen

Zu den IT-Umgebungen im Gesundheitswesen gehören lokale Systeme, Cloud-Plattformen sowie spezialisierte klinische Anwendungen. Die Gewährleistung einer sicheren Interoperabilität zwischen diesen Systemen, etwa zwischen der elektronischen Patientenakte (ePA) und Bildgebungsplattformen, führt zu einer hohen technischen Komplexität.

Viele Einzellösungen und ein ineffizienter Betrieb

Für Backups, Sicherheit und Verwaltung nutzen viele MSPs derzeit noch verschiedene separate Tools. Dieser Ansatz erhöht den Betriebsaufwand, führt zu Sicherheitslücken und beeinträchtigt die Reaktionsfähigkeit bei Vorfällen.

[2] IBM. (2025). Cost of a Data Breach Report 2025: The AI Oversight Gap. IBM & Ponemon Institute.

[3] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). (2024). 2024 Internet Crime Report.

[4] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). (2025). 2025 Internet Crime Report.

Herausforderungen für Branche und Betrieb

Abgesehen von den technischen Herausforderungen ist eine Zusammenarbeit mit Gesundheitseinrichtungen mit strengen regulatorischen und betrieblichen Anforderungen verbunden.

Strenge Compliance-Vorschriften und Audits

MSPs müssen strenge Compliance-Anforderungen erfüllen und sind in der Regel auch dafür haftbar. Dabei sind Audit-Readiness und Dokumentation von entscheidender Bedeutung. Die Erfüllung dieser Anforderungen kann jedoch die Ressourcen von MSPs stark belasten.

Datenintegrität und Vertrauen

Gesundheitseinrichtungen sind dafür verantwortlich, die Richtigkeit und Integrität von medizinischen Daten sicherzustellen. Stille Datenkorruption und inkonsistente Aufzeichnungen bergen das ernstzunehmende Risiko von Fehldiagnosen. MSPs müssen dieses Risiko minimieren.

Bildgebungssysteme und Datenverfügbarkeit

Medizinische Bildgebungssysteme erzeugen riesige Datensätze, die jederzeit und sofort verfügbar sein müssen. MSPs müssen daher hybride Architekturen entwerfen, die Verfügbarkeit und sichere Speicherung optimal ausbalancieren.

Kostenzwänge

Obwohl die Sicherheitsanforderungen steigen, verfügen Gesundheitseinrichtungen oft nur über begrenzte IT-Budgets. MSPs müssen daher ein hohes Schutzniveau bieten und gleichzeitig kosteneffizient arbeiten.

Eine Plattform, die speziell für MSPs im Gesundheitswesen entwickelt wurde

Um im Gesundheitswesen erfolgreich zu sein, benötigen MSPs eine Plattform, die Sicherheit, Data Protection und effiziente Betriebsabläufe in einer einzigen Lösung vereint. Die Acronis Cyber Platform bietet MSPs die Möglichkeit, die gesamte klinische Umgebung umfassend zu schützen, ihre Betriebsabläufe zu vereinfachen und ihre Rentabilität zu steigern.

Mit der Acronis Cyber Platform können MSPs Folgendes erreichen:

Garantierte Kontinuität des Klinikbetriebs

- Extrem hohe Verfügbarkeit kritischer Systeme durch sofortige Wiederherstellung und RTOs von nahezu null
- Kontinuierlicher Zugriff auf ePAs, Bildgebungssysteme und medizinische Geräte am Patientenbett – auch während eines Cyberangriffs

Schutz für die gesamte Umgebung

- Schutz moderner Cloud-Plattformen und älterer medizinischer Systeme über einen einzigen integrierten Agenten
- Risikominimierung durch Schutz von Endpunkten, Workloads und IoMT-Geräten (Internet of Medical Things)

Einfachere Compliance und Audit-Readiness

- Automatisierung von Compliance-Verfahren mittels Data Protection-Karten und auditfähigen Berichte
- Übergang von Standard-IT-Services zu margenstarken Compliance-Angeboten

Zuverlässige und sichere Wiederherstellung

- Malwarefreie Datenwiederherstellung dank sicherer Wiederherstellungsfunktionen
- Überprüfung und Bereinigung von Backup-Daten vor der Wiederherstellung

Geringere Komplexität und höhere Margen

- Ablösung mehrerer Einzellösungen für Backup, Sicherheit und Verwaltung durch eine einzige All-in-one-Plattform
- Höhere Technikereffizienz und höhere Gewinne

Acronis Cyber Platform: Funktionen speziell für das Gesundheitswesen

Acronis bietet ein umfassendes Spektrum speziell für das Gesundheitswesen entwickelter Funktionen:

Einheitliche Cyber Protection-Plattform: Acronis vereint Cyber Security, Data Protection, Disaster Recovery und Endpunktverwaltung in einer einzigen Plattform. Dadurch wird der tägliche Betrieb erheblich vereinfacht und die Transparenz deutlich verbessert.

Advanced Backup und Recovery: Mithilfe imagebasierter Backups, unveränderlicher Speicherung und einer sofortigen Wiederherstellung können MSPs kritische klinische und bildgebende Systeme zuverlässig schützen.

Endpunktschutz und EDR: Mit EDR (Endpoint Detection and Response) können MSPs Workstations, Server und Remote-Endpunkte in Gesundheitseinrichtungen absichern.

Automatisierte Compliance und Data Protection: Die Acronis Cyber Platform ermöglicht es MSPs mithilfe automatisierter Erkennungstools, sensible Gesundheitsdaten zu identifizieren und zu schützen. Ein zentrales Reporting-Tool stellt zudem die Audit-Readiness sicher.

Microsoft 365-Schutz: Da viele Gesundheitseinrichtungen die beliebte Produktivitäts-suite nutzen, können MSPs die kontinuierliche Verfügbarkeit von Microsoft 365-Daten und -Apps sowie anderer Kommunikations- und Kollaborationstools wie E-Mail, Dateispeicher und Plattformen zur Patientenkoordination sicherstellen.

Unterstützung für Legacy-Systeme: MSPs können den Schutz auf ältere Betriebssysteme und spezielles medizinisches Equipment ausweiten, ohne dass dafür störende Upgrades erforderlich sind.

Forensische Backups und Datenintegrität: MSPs können forensische Daten zur Untersuchung von Vorfällen erfassen und mithilfe blockchainbasierter Verifizierungstechnologien die Integrität von Datensätzen sicherstellen.

Vorteile der Acronis Cyber Platform

Acronis bietet eine speziell für das Gesundheitswesen entwickelte, nativ integrierte Plattform mit einer zentralen Management-Konsole. Diese eröffnet MSPs folgende Vorteile, die ein Flickenteppich aus Einzellösungen nicht bieten kann:

- Bereitstellung umfassender Cyber Protection für alle Arten von medizinischen Umgebungen
- Weniger Betriebsaufwand, weniger Kosten und weniger Einzellösungen
- Bessere Reaktionszeiten und Recovery-KPIs
- Erweiterung des Portfolios um margenstarke Compliance- und Sicherheitsservices
- Margensteigerung trotz Skalierung von Services

Da alle wichtigen Funktionen auf einer einzigen Plattform zusammengeführt sind, können MSPs ihre Kosten senken, ihre Abläufe vereinfachen und gleichzeitig das hohe Maß an Resilienz gewährleisten, das von Gesundheitseinrichtungen gefordert wird.

Steigen Sie in die Gesundheitsbranche ein

Um Kontinuität, Sicherheit und Compliance zu gewährleisten, sind Gesundheits-einrichtungen auf vertrauenswürdige Partner angewiesen. Mit der Acronis Cyber Platform können MSPs diese Geschäftschance erfolgreich nutzen.

↘ Buchen Sie eine Demo und sehen Sie selbst, wie Acronis MSPs im Gesundheitswesen unterstützt

↘ Testen Sie die Plattform und bieten Sie Resilienzlösungen für das Gesundheitswesen an

Acronis

Erfahren Sie mehr auf acronis.com